UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/774,674	02/01/2001	Helena Handschuh	032326-118	3521

7590 08/12/2004

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
LIPMAN, JACOB	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/774,674	HANDSCHUH, HELENA	
	Examiner	Art Unit	
	Jacob Lipman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 2, and 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Miyazaki et al., Japanese Patent number 411317734A and US Patent number 6,477,254 (referenced columns).

With regard to claims 1 and 13, Miyazaki discloses an countermeasure method using a public key cryptography based on elliptic curves (column 2 lines 21-23) by generating a random number the same size as the secret key (column 3 lines 43-46) performing a scalar multiplication on the random number and the secret key (column 3 lines 47-50), calculation a second scalar multiplication with the random number and a point on the curve (column 4 lines 55-58).

With regard to claim 2, Miyazaki discloses calculating a new integer at each execution (column 3 lines 40-42).

3. Claims 1, 2, and 13 are rejected under 35 U.S.C. 102(b) as being unpatentable over Kocher et al., in Differential Power Analysis, on the Internet since 1998.

With regard to claims 1, 2, and 13, Kocher discloses a method to prevent DPAs is to update the key with a random hashing, and to use counters to prevent attackers from gathering a large number of samples (page 9 paragraph 2).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz, in A Course in Number Theory and Cryptography, in view of Miyazaki.

With regard to claims 7 and 8, Miyazaki discloses the method as outlined above, but does not mention doubling points. Koblitz discloses doubling points in elliptic curve cryptography speeds up decryption (pages 178-179). It would have been obvious to double the points in Miyazaki to speed up decryption.

With regard to claims 3-6 and 9-12, Miyazaki discloses the method as outlined above, but does not mention keeping the same number for a number of executions. The examiner takes official notice that having keeping the same number for a number of executions would lower processing requirements. It would have been obvious for one of ordinary skill in the art to reuse the same integer for a given number of executions to lower processing needs.

6. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kobitz in view of Kocher.

With regard to claims 7 and 8, Kocher discloses the method as outlined above, but does not mention doubling points. Koblitz discloses doubling points in elliptic curve

cryptography speeds up decryption (pages 178-179). It would have been obvious to double the points in Kocher to speed up decryption.

With regard to claims 3-6 and 9-12, Kocher discloses the method as outlined above, but does not mention keeping the same number for a number of executions. The examiner takes official notice that having keeping the same number for a number of executions would lower processing requirements. It would have been obvious for one of ordinary skill in the art to reuse the same integer for a given number of executions to lower processing needs.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob Lipman whose telephone number is 703-305-0716. The examiner can normally be reached on 7:00 - 4:00 (M-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

JL